SUCCESS STORY

SBA-K1
SBA Research GmbH

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Centre (K1)

Type of project: Secure & Sustainable Distributed Systems, strateg.

SECURE RANDOM NUMBERS IN DISTRIBUTED SYSTEMS

DEVELOPMENT OF TWO PROTOCOLS FOR RANDOM NUMBER GENERATION: LESS RESOURCE CONSUMPTION, MORE SECURITY, AND BETTER APPLICABILITY IN CLOSED SYSTEMS

Public distributed ledgers are playing an increasingly important role in our lives. One of the frontrunners of these systems is Bitcoin, a digital currency that is generated and managed independently of central bodies. However, there are now countless projects, platforms and applications that go far beyond the functionality of a payment system. Despite advancing technical innovation, many of these systems are still based on the proof-of-work principle, which is already used for Bitcoin. However, this principle leads to enormous resource consumption and is not feasible in the case of compartmentalized networks (such as in corporate networks). Energy-efficient alternatives including Proof-of-Stake or traditional Byzantine Fault Tolerant (BFT) protocols often rely heavily on the distributed generation of random numbers, for example to implement the leader selection process.

Random numbers are also important in other domains: in order to obtain representative results in surveys, interviewees must be randomly selected for the extrapolation to produce a correspondingly meaningful result. However, if these data points are not randomly selected, this can influence the results of the surveys. In addition, the selection itself often cannot be verified, potentially posing a security risk (similar to the situation of whether I can see what number the other person rolls in a dice game or have to rely on their statement).

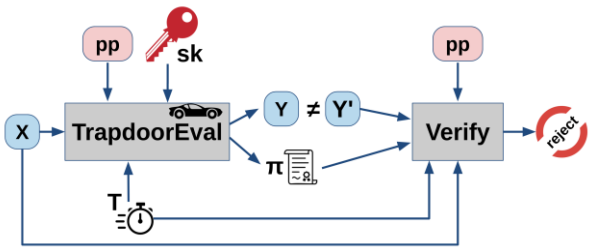
Federal Ministry
Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry
Republic of Austria
Digital and Economic Affairs

Version 01/2020

SUCCESS STORY

With our HydRand[1] protocol we were able to improve theoretical efficiency compared to other designs with similar guarantees and demonstrated – through a prototype implementation – that these results can be translated into practice. RandRunner[2], our second protocol, further reduces the communication overhead through a minimalistic design, leading to higher scalability and more diverse applications. It ensures the creation of a new random value, with only a single message distributed through the network. In addition, the protocol provides many important security guarantees and desired features, for example the ability to automatically resume operation after a network failure.



Schematic representation of the core cryptographic component of the RandRunner protocol: Trapdoor-VDF with Strong Uniqueness (©Philipp Schindler)

Impact and effects

Our corporate partners benefit from these new protocols not only in the area of digital ledgers, but have a new method at their disposal to implement distributed systems securely and energy-efficiently at the enterprise level. Other potential applications for HydRand and RandRunner include, for example, fair resource allocation problems such as the selection of applicants for kindergarten (in order to prevent bias on the part of the authority), the aforementioned selection of survey participants, or other statistical evaluations based on a random selection of data.

Project coordination (Story)
Philipp Schindler
Researcher
SBA Research

T +43 (1) 505 36 88
pschindler@sba-research.org

SBA-K1
SBA Research gGmbH
Floragasse 7, 5. OG
1040 Wien
T +43 (0) 664 4111588
mklemen@sba-research.org
www.sba-research.org

This success story was provided by the centre management for the purpose of being published on the FFG website. SBA-K1 is a COMET-Centre within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the City of Vienna. The COMET Programme is managed by FFG. Further information on COMET: www.ffg.at/comet

[1] P.Schindler, A. Judmayer, N. Stifter, and E. Weippl. HydRand: Efficient Continuous Distributed Randomness. In 2020 IEEE Symposium on Security and Privacy (SP 2020)

[2] P. Schindler, A. Judmayer, M. Hittmeir, N. Stifter, and E. Weippl. RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness. In 28th Annual Network and Distributed System Security Symposium (NDSS 2021). The Internet Society, February 2021.

Federal Ministry
Republic of Austria
Climate Action, Environment, Energy, Mobility, Innovation and Technology

Federal Ministry
Republic of Austria
Digital and Economic Affairs

Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at